Cassandra Crossing 642/ Il Q-day non ci sarà

(642)—La catastrofe quantistica descritta da Cassandra è una certezza, ma è anche certo il che il Q-Day non ci sarà. Vediamo insieme…

Cassandra Crossing 642/ Il Q-day non ci sarà



(642)—La catastrofe quantistica descritta da Cassandra è una certezza, ma è anche certo che il Q-Day non ci sarà. Vediamo insieme perché.

6 ottobre 2025—In un recente articolo, Cassandra aveva parlato di Apocalisse Quantistica, vaticinando (è un piacere vincere facile!) che la disponibilità dei primi computer quantistici provocherà un terremoto perché la crittografia attuale può essere decrittata rapidamente da un computer quantistico che usi il già noto algoritmo di Shor, od uno degli altri ormai disponibili o segretamente realizzati.

Insomma, parliamo di una crisi che investirà tutta Internet e tutte le applicazioni del digitale che utilizzano la crittografia. Molto in alto su questa lista ci sono le criptovalute, ed in particolare Bitcoin ed Ethereum, oggetto di una seconda esternazione di Cassandra.

Il giorno di inizio di questa apocalisse, semplicisticamente definito come quello della disponibilità di un computer quantistico sufficientemente grande e stabile da poter girare calcoli reali, è stato battezzato Quantum Day, o per brevità Q-Day.

Ecco, non è purtroppo una rassicurazione, ma il Q-Day non ci sarà. Mentre le "piaghe" tecnologiche dell'apocalisse quantistica previste da molti, si avvereranno tutte, insieme ad altre non ancora prevedibili.

Onde prevenire la sollevazione dei 24 impazienti lettori, spieghiamo subito il perché.

Veniamo quindi subito al punto.

Lasciando perdere la gente comune, **nessuno degli attori coinvolti** nella ricerca, nell'industrializzazione, nella produzione e nello sfruttamento del calcolo quantistico, **ha l'interesse di annunciare, dimostrandolo, il possesso di un computer quantistico realmente utilizzabile** per calcolo quantistico, e **dichiarare così raggiunto il Q-Day**.

Nessuno!

"*Ma perché allora sulla stampa escono continuamente notizie di grandi aziende che annunciano grandi progressi nella realizzazione di un computer quantistico?*" esclameranno i 24 impazienti lettori.

Semplice, per un'azienda fare annunci sui piccoli "progressi" compiuti (veri o presunti) verso la realizzazione di un computer quantistico è un ottimo modo per far salire le proprie quotazioni azionarie e "pompare" la propria reputazione. Nessuno si sottrae a questo giochetto.

Ma aver già realizzato un computer quantistico, per qualsiasi attore che ci riesca, è un fatto che conviene tenere assolutamente segreto finché possibile.

Perché?

Molti dei 24 intrepidi lettori avranno già preceduto Cassandra, immaginandosi parecchi esempi; forse proprio procedere per esempi è la cosa migliore.

Supponiamo che un Crypto Mogul (ce ne sono tanti) venga in possesso di un computer quantistico funzionante. Tutti i wallet e le blockchain diventeranno da lui controllabili, ma impossessarsi semplicemente dei capitali lo lascerebbe con un pugno di mosche in mano, visto che il valore delle crypto (quelle già possedute e quelle di cui potrebbe impossessarsi) precipiterebbe immediatamente a zero.

Dovrebbe invece agire nel segreto, progettare i suoi furti nella maniera più soft possibile, impossessandosi di bitcoin fermi da tempo, ma non sospettabili come i wallet attribuiti a Satoshi Nakamoto, e senza esagerare.

Infatti, il movimento degli enormi wallet "congelati" nella blockchain sarebbe proprio un indizio rivelatore del possesso di un computer quantistico, e potrebbe generare quel crypto-panico che il lestofante quantistico vorrebbe evitare a tutti i costi, per mantenere il proprio vantaggio. E non sarebbe una cosa facile.

Ma veniamo ad un esempio ancora più grande e convincente; la rivelazione dei dati criptati e riservati che molte superpotenze stanno da anni memorizzando in attesa di poterli decodificare.

Anche dati vecchi di mesi o di anni possono essere preziosi per l'intelligence e lo spionaggio, e per questo vengono intercettati e messi da parte da tutte le superpotenze.

Corrispondenza riservata, piani militari, documenti tecnici segreti, ma anche chiavi crittografiche, credenziali di accesso e chi più ne ha più ne metta. Un vero tesoro digitale, chiuso in un cofano impenetrabile, per il quale si attende il grimaldello quantistico che, prima o poi, arriverà.

E cosa dire dell'uso dei dati decriptati, come le credenziali di accesso, per compiere atti di sabotaggio elettronico o di guerra elettronica? Avendo improvvisamente accesso ai dati del sistema finanziario globale, e potendo progettare l'azione con anni di anticipo, bloccarlo od addirittura prendere il controllo di alcune parti di esso rientra nel novero del possibile.

Cassandra potrebbe continuare, ma lascia questo ai suoi 24 interessatissimi lettori come compito a casa.

Torniamo quindi alla tesi iniziale: che vantaggio avrebbe la parte che ottenesse per prima l'accesso ad un computer quantistico funzionante, a rivelare che il Q-Day è arrivato?

Evidentemente nessuno, questo annullerebbe tutti quei vantaggi strategici e commerciali che il possesso della tecnologia offrirebbe.

E per cosa dovrebbe farlo? Un ipotetico vantaggio commerciale? Il premio Nobel?

Se anche questa tentazione venisse a qualcuna delle persone coinvolte, il bavaglio del segreto militare, del "Bene del Paese" e della "Lotta contro il Male" prevarrebbe, e certamente queste voci sono state già zittite, preventivamente, ed occorrendo lo saranno anche successivamente.

La profezia di oggi è quindi facile:

Niente Q-Day, ma solo l'inizio di attività sotterranee volte ad ottenere risultati politici, strategici ed economici, senza rivelare, per il periodo più lungo possibile, il possesso dell'arma finale".

Solo l'avverarsi di fatti "strani", come il ricordato movimento di criptovalute ferme da anni nelle blockchain, imprevedibili vantaggi geopolitici od atti ostili cibernetici di grandissimo "successo" **saranno indizi rivelatori dell'avvenuta "supremazia quantistica"** raggiunta da qualche paese od organizzazione.

Supremazia che, come avvenuto per le armi atomiche, verrà prima o poi neutralizzata dal raggiungimento dello stesso obbiettivo da parte di altri; sperabilmente, senza che nel frattempo rivolgimenti globali e guerre cibernetiche abbiano creato danni planetari.

A questo punto una domanda sorge spontanea; **ci sono già indizi che questo stia accadendo oggi?**

Che qualcuno abbia già raggiunto almeno la fase iniziale della supremazia quantistica?

Per ora solo pochissimi e molto vaghi. Alcuni grossi capitali, immobili da anni, hanno in effetti iniziato a "muoversi" nella blockchain di Bitcoin. Capitali grossi, ma piccoli rispetto al valore complessivo di Bitcoin.

L'indizio per ora più rivelatore, a parere di Cassandra, è proprio il fatto che **pubblicamente si faccia ancora così poco per sostituire gli algoritmi crittografici attuali con algoritmi crittografici post-quantistici** (già oggi disponibili) in tutto il sistema digitale planetario.

Queste attività sembrano per ora essere considerate non un'emergenza, ma solo un interessante ed importante settore di ricerca.

Niente di più.

Nessuna emergenza informatica planetaria è stata dichiarata. Nessuna grande attività di aggiornamento informatico come quella dello Y2K (più noto come "bug del millennio") è in fase di realizzazione. Perché il quasi panico dell'Y2K non si ripete su una scala molto maggiore?

Strano, vero?

Aggiornare tutti gli algoritmi oggi usati è certamente un'attività enorme e molto difficile, ma proprio per questo tutti avrebbero l'interesse a cominciare subito per terminare il più rapidamente possibile, prima che qualcuno raggiunga la supremazia quantistica.

Certamente, dove conta, queste attività di irrobustimento digitale sono già da tempo in corso; ma niente avviene a livello pubblico.

Ecco, su questa stranezza sarebbe possibile elaborare ulteriormente considerazioni interessanti, **anche se ahimè molto simili a teorie del complotto**.

Ad esempio, che dove si prendono le decisioni importanti, **ci sia un interesse comune a non creare il panico**. Che, proprio come avviene per gli arsenali cibernetici, **convenga a tutti non rivelare la supremazia o la deficienza dei propri**.

Un giorno tutte queste ipotesi diverranno storia, e **si vedrà se nel cavallo di legno c'era davvero qualcosa di strano**; speriamo solo che rimanga qualcuno per leggerla, e che questa storia non si riduca effettivamente ad un tesoro, ma solo archeologico, riservato ai primi alieni in visita.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

***Licenza d'utilizzo**: i contenuti di questo articolo, dove non diversamente indicato, sono sotto licenza Creative Commons Attribuzione—Condividi allo stesso modo 4.0 Internazionale (CC BY-SA 4.0),* tutte le informazioni di utilizzo del materiale sono disponibili a questo link*.*

By Marco A. L. Calamari on October 8, 2025.

Canonical link

Exported from Medium on March 30, 2026.